CHAPTER

Domain 4: Communication and network security

4

CHAPTER OUTLINE

INTRODUCTION

Communications and network security are fundamental to our modern life. The Internet, the World Wide Web, online banking, instant messaging, email, and many other technologies rely on network security; our modern world cannot exist without it.

Eleventh Hour CISSP®. http://dx.doi.org/10.1016/B978-0-12-811248-9.00004-8

Copyright © 2017 Elsevier Inc. All rights reserved.

Communications and network security focuses on the confidentiality, integrity, and availability of data in motion.

Communications and Network Security is one of the largest domains in the Common Body of Knowledge and contains more concepts than any other domain. This domain is also one of the most technically deep domains, requiring technical knowledge including *packets, segments, frames*, and their headers. The ability to understand this domain is critical for exam success.

NETWORK ARCHITECTURE AND DESIGN

Our first section is network architecture and design. We will discuss how networks should be designed and the controls they may contain, focusing on deploying defense-in-depth strategies and weighing the cost and complexity of a network control versus the benefit provided.

FUNDAMENTAL NETWORK CONCEPTS

Before we can discuss specific Communications and Network Security concepts, we need to understand the fundamental concepts behind them. Terms like *broadband* are often used informally; the exam requires a precise understanding of information security terminology.

Simplex, half-duplex, and full-duplex communication

Simplex communication is one-way, like a car radio tuned to a music station. *Half-duplex* communication sends or receives at one time only, not simultaneously, like a walkie-talkie. *Full-duplex* communications send and receive simultaneously, like two people having a face-to-face conversation.

LANs, WANs, MANs, GANs, and PANs

A *LAN* is a local-area network. A LAN is a comparatively small network, typically confined to a building or an area within a building. A *MAN* is a metropolitan area network, which is typically confined to a city, a ZIP code, a campus, or office park. A *WAN* is a wide area network, typically covering cities, states, or countries. A *GAN* is a global area network, which is a global collection of WANs.

At the other end of the spectrum, the smallest of these networks are PANs: personal area networks, with a range of 100 m or much less. Low-power wireless technologies like Bluetooth use PANs.

Internet, Intranet, and Extranet

The *Internet* is a global collection of peered networks running transmission control protocol/Internet protocol (TCP/IP), providing best effort service. An *Intranet* is a privately owned network running TCP/IP, such as a company network. An *Extranet* is a connection between private Intranets, such as connections to business partner intranets.

Circuit-switched and packet-switched networks

The original voice networks were circuit-switched, in that a circuit or channel (ie, a portion of a circuit) was dedicated between two nodes. *Circuit-switched networks* can provide dedicated bandwidth to point-to-point connections, such as a T1 connecting two offices.

One drawback of circuit-switched networks is that once a channel or circuit is connected, it is dedicated to that purpose, even if no data is being transferred. Packet-switched networks were designed to address this issue, as well as handle network failures more robustly.

Instead of using dedicated circuits, packet-switched networks break data into packets, each sent individually. If multiple routes are available between two points on a network, packet switching can choose the best route and fall back to secondary routes in case of failure. Packets may take any path across a network and are then reassembled by the receiving node. Missing packets can be retransmitted and out-of-order packets can be resequenced.

Unlike circuit-switched networks, packet-switched networks make unused bandwidth available for other connections. This can give packet-switched networks a cost advantage over circuit-switched networks.

Quality of service

Making unused bandwidth available for other applications presents a challenge: What happens when all bandwidth is consumed? Which applications "win" the required bandwidth? This is not an issue with circuit-switched networks, where applications have exclusive access to dedicated circuits or channels.

Packet-switched networks may use quality of service (QoS) to give specific traffic precedence over other traffic. For example: QoS is often applied to voice over Internet protocol (VoIP) traffic (ie, voice via packet-switched data networks) to avoid interruption of phone calls. Less time-sensitive traffic, such as simple mail transfer protocol (SMTP), a store-and-forward protocol used to exchange email between servers that often receives a lower priority. However, small delays in email exchange are less likely to be noticed as opposed to dropped phone calls.

THE OSI MODEL

The OSI (open system interconnection) reference model is a layered network model. The model is abstract; we do not directly run the OSI model in our systems (most now use the TCP/IP model). Rather, it is used as a reference point, so "Layer 1" (physical) is universally understood, whether you are running Ethernet or ATM, for example. "Layer X" in this book refers to the OSI model.

The OSI model has seven layers, as shown in Table 4.1. The layers may be listed in a top-to-bottom or bottom to top order. Using the latter, they are *Physical, Data Link, Network, Transport, Session, Presentation, and Application*.

Layer 1: Physical

Physical is layer 1 of the OSI model. This first layer describes units of data such as *bits* represented by energy (such as light, electricity, or radio waves) and the medium

Table 4.1 The OSI Model

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical

used to carry them, such as copper or fiber optic cables. WLANs have a physical layer, even though we cannot physically touch it.

Cabling standards such as *thinnet, thicknet*, and unshielded twisted pair (UTP) exist in layer 1, among many others devices, including hubs and repeaters.

Layer 2: Data link

The data link layer handles access to the physical layer as well as LAN communication. An *Ethernet* card and its *media access control (MAC)* address are at layer 2, as are switches and bridges.

Layer 2 is divided into two sublayers: media access control (MAC) and logical link control (LLC). The MAC layer transfers data to and from the physical layer, while LLC handles LAN communications. MAC touches layer 1 and LLC touches layer 3.

Layer 3: Network

The network layer describes routing, which is moving data from a system on one LAN to a system on another. IP addresses and routers exist at layer 3, where protocols include IPv4 and IPv6, among others.

Layer 4: Transport

The transport layer handles packet sequencing, flow control, and error detection. TCP and user datagram protocol (UDP) are layer 4 protocols.

Layer 4 makes a number of features available, such as resending or resequencing packets. Taking advantage of these features is a protocol implementation decision. As we will see later, TCP takes advantage of these features, at the expense of speed. Many of these features are not implemented in UDP, which chooses speed over reliability.

Layer 5: Session

The session layer manages sessions, which provide maintenance on connections. Mounting a file share via a network requires a number of maintenance sessions, such as remote procedure calls (RPCs), which exist at the session layer. The session layer provides connections between applications and uses simplex, half-duplex, and full-duplex communication.

EXAM WARNING

The transport and session layers are often confused. For example, is "maintenance of connections" a transport layer or session layer issue? Packets are sequenced at the transport layer, and network file shares can be remounted at the session layer; you may consider either to be maintenance. Words like "maintenance" imply more work than packet sequencing or retransmission; it requires "heavier lifting," like remounting a network share that has been unmounted, so session layer is the best answer.

Layer 6: Presentation

The presentation layer presents data to the application and user in a comprehensible way. Presentation layer concepts include data conversion, characters sets such as ASCII, and image formats such as GIF (graphics interchange format), JPEG (joint photographic experts group), and TIFF (tagged image file format).

Layer 7: Application

The application-layer is where you interface with your computer application. Your web browser, word processor, and instant messaging client exist at layer 7. The protocols Telnet and FTP are application-layer protocols.

THE TCP/IP MODEL

The TCP/IP is a popular network model created by DARPA in the 1970s. TCP/IP is an informal name (named after the first two protocols created); the formal name is the Internet Protocol Suite. The TCP/IP model is simpler than the OSI model, as shown in Table 4.2.

While TCP and IP receive top billing, TCP/IP is actually a suite of protocols including UDP (user datagram protocol) and ICMP (internet control message protocol), among many others.

Network access layer

The network access layer of the TCP/IP model combines layers 1 (physical) and 2 (data link) of the OSI model. It describes layer 1 issues such as energy, bits, and the

Table 4.2 The OSI Model vs TCP/IP Model

	OSI Model	TCP/IP Model
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Host-to-host transport
3	Network	Internet
2	Data link	Network access
1	Physical	

medium used to carry them (copper, fiber, wireless, etc.). It also describes layer 2 issues like converting bits into protocol units such as Ethernet frames, MAC addresses, and network interface cards (NICs).

Internet layer

The Internet layer of the TCP/IP model aligns with the layer 3 (network) layer of the OSI model. This is where IP addresses and routing live. When data is transmitted from a node on one LAN to a node on a different LAN, the Internet layer is used. IPv4, IPv6, ICMP, and routing protocols (among others) are Internet layer TCP/IP protocols.

Host-to-host transport layer

The *Host-to-Host Transport layer* is sometimes called either "Host-to-Host" or, more commonly, "Transport"; this book will use "Transport." It connects the Internet layer to the application-layer. It is where applications are addressed on a network via ports. TCP and UDP are the two transport layer protocols of TCP/IP.

Application-layer

The TCP/IP application-layer combines layers 5–7 (session, presentation, and application) of the OSI model. Most of these protocols use a client-server architecture, where a client (eg, *ssh*) connects to a listening server (called a daemon on UNIX systems), such as sshd. The clients and servers use either TCP or UDP (and sometimes both) as a transport layer protocol. TCP/IP application-layer protocols include secure shell (SSH), *Telnet,* and *FTP*, among many others.

MAC addresses

A MAC address is the unique hardware address of an Ethernet NIC, typically "burned in" at the factory. MAC addresses may be changed in software.

DID YOU KNOW?

Historically, MAC addresses are 48 bits long. They have two halves: the first 24 bits form the Organizationally Unique Identifier (OUI) and the last 24 bits form a serial number (formally called an extension identifier).

EUI-64 MAC addresses

The IEEE created the EUI-64 (extended unique identifier) standard for 64-bit MAC addresses. The OUI is still 24 bits, but the serial number is 40 bits. This allows for far more MAC addresses, compared with 48-bit addresses. *IPv6 autoconfiguration* is compatible with both types of MAC addresses.

IPv4

IPv4 is Internet protocol version 4, commonly called "IP." It is a simple protocol, designed to carry data across networks. It is so simple that it requires a "helper protocol" called ICMP (see later). IP is connectionless and unreliable; it provides "best

effort" delivery of packets. If connections or reliability are required, they must be provided by a higher-level protocol carried by IP, such as TCP.

IPv4 uses 32-bit source and destination addresses, usually shown in "dotted quad" format, such as "192.168.2.4." A 32-bit address field allows 2^{32}, or nearly 4.3 billion, addresses.

IPv6

IPv6 is the successor to IPv4, featuring far larger address space (128-bit addresses compared to IPv4's 32 bits), simpler routing, and simpler address assignment. A lack of IPv4 addresses was the primary factor that led to the creation of IPv6.

DID YOU KNOW?

Most modern systems are "dual stack" and use both IPv4 and IPv6 simultaneously. Hosts may also access IPv6 networks via IPv4; this is called tunneling.

TCP

TCP is a reliable layer 4 protocol. TCP uses a three-way handshake to create reliable connections across a network. TCP can reorder segments that arrive out-of-order and retransmit missing segments.

TCP ports

TCP connects from a source port to a destination port, such as from source port 51178 to destination port 22. The TCP port field is 16 bits, allowing port numbers from 0 to 65,535.

There are two types of ports, *reserved* and *ephemeral*. A reserved port is 1023 or lower; ephemeral ports are 1024-65,535. Most operating systems require super-user privileges to open a reserved port. Any user may open an (unused) ephemeral port.

UDP

UDP is a simpler and faster cousin to TCP. UDP is commonly used for applications that are "lossy" (can handle some packet loss), such as streaming audio and video. It is also used for query-response applications, such as DNS queries.

ICMP

Internet control message protocol, or ICMP, is a helper protocol that assists layer 3. ICMP is used to troubleshoot and report error conditions; without ICMP to help, IP would fail when faced with routing loops, ports, hosts, or networks that are down, among other issues. ICMP has no concept of ports, as TCP and UDP do, but instead uses types and codes.

APPLICATION-LAYER TCP/IP PROTOCOLS AND CONCEPTS

A multitude of protocols exist at TCP/IP's application-layer, which combines the session, presentation, and application-layers of the OSI model.

Telnet

Telnet provides terminal emulation over a network. "Terminal" means text-based VT100-style terminal access. Telnet servers listen on TCP port 23. Telnet was the standard way to access an interactive command shell over a network for over 20 years.

Telnet is weak because it provides no confidentiality; all data transmitted during a Telnet session is plaintext, including the username and password used to authenticate to the system.

FTP

FTP is the file transfer protocol, used to transfer files to and from servers. Like Telnet, FTP has no confidentiality or integrity and should not be used to transfer sensitive data over insecure channels.

FTP uses two ports. The control connection, where commands are sent, is TCP port 21. "Active FTP" uses a data connection, where data is transferred, that originates from TCP port 20. Here are two socket pairs; the next two examples use arbitrary ephemeral ports:

- Client: 1025 → Server: 21 (Control Connection)
- Server: 20 → Client: 1026 (Data Connection)

Notice that the data connection originates from the server, in the opposite direction of the control channel. This breaks classic client-server data flow direction. Many firewalls will block the active FTP data connection for this reason, breaking active FTP. Passive FTP addresses this issue by keeping all communication from client to server:

- Client: 1025 → Server: 21 (Control Connection)
- Client: 1026 → Server: 1025 (Data Connection)

Passive FTP is more likely to pass through firewalls cleanly, since it flows in classic client-server direction.

SSH

Secure shell (SSH) was designed as a secure replacement for Telnet, FTP, and the UNIX "R" commands (rlogin, rshell, etc.). It provides confidentiality, integrity, and secure authentication, among other features. SSH includes SFTP (SSH FTP) and SCP (secure copy) for transferring files. SSH can also be used to securely tunnel other protocols, such as HTTP. SSH servers listen on TCP port 22 by default.

SMTP, POP, and IMAP

SMTP is the simple mail transfer protocol, which is used to transfer email between servers. SMTP servers listen on TCP port 25. *POP*v3 (post office protocol) and *IMAP* (Internet message access protocol) are used for client-server email access, which use TCP ports 110 and 143, respectively.

DNS

DNS is the domain name system, a distributed global hierarchical database that translates names to IP addresses, and vice versa. DNS uses both TCP and UDP; small responses use UDP port 53, while large responses, including zone transfers, use TCP port 53.

HTTP and HTTPS

Hypertext transfer protocol, or HTTP, transfers unencrypted web-based data. HTTPS (hypertext transfer protocol secure) transfers encrypted web-based data via SSL/*TLS* (see Section "SSL/TLS", later). HTTP uses TCP port 80, and HTTPS uses TCP port 443. HTML (hypertext markup language) is used to display web content.

LAN TECHNOLOGIES AND PROTOCOLS

LAN concepts focus on layers 1–3 technologies such as network cabling types, physical and logical network topologies, Ethernet, FDDI, and others.

Ethernet

Ethernet operates at layer 2 and is a dominant local-area networking technology that transmits network data via frames. Ethernet is baseband (ie, one channel), so it must address issues such as collisions, where two nodes attempt to transmit data simultaneously.

WAN TECHNOLOGIES AND PROTOCOLS

ISPs and other "long-haul" network providers, whose networks span from cities to countries, often use WAN technologies. Many of us have hands-on experience configuring LAN technologies such as connecting Cat5 network cabling; it is less common to have hands-on experience building WANs.

T1s, T3s, E1s, and E3s

There are a number of international circuit standards; the most prevalent are T Carriers (United States) and E Carriers (Europe).

FAST FACTS

Here is a summary of common circuits:

- A **T1** is a dedicated 1.544-megabit circuit that carries 24.64 kbit/s DS0 (Digital Signal 0) channels.
- A **T3** is 28 bundled T1s, forming a 44.736-megabit circuit.
- An **E1** is a dedicated 2.048-megabit circuit that carries 30 channels.
- An **E3** is 16 bundled E1s, forming a 34.368-megabit circuit.

Frame Relay

Frame Relay is a packet-switched layer 2 WAN protocol that provides no error recovery and focuses on speed. Higher-layer protocols carried by Frame Relay, such as TCP/IP, can be used to provide reliability.

Frame Relay multiplexes multiple logical connections over a single physical connection, which create virtual circuits. This shared bandwidth model is an alternative to dedicated circuits such as T1s. A PVC (permanent virtual circuit) is always connected and is analogous to a real dedicated circuit like a T1. A switched virtual circuit (SVC) sets up each "call," transfers data, and terminates the connection after an idle timeout.

MPLS

Multiprotocol label switching (MPLS) provides a way to forward WAN data using labels via a shared MPLS cloud network. Decisions are based on the labels, not on encapsulated header data (such as an IP header). MPLS can carry voice and data and can be used to simplify WAN routing.

CONVERGED PROTOCOLS

"Convergence" is a recent network buzzword. It means providing services such as industrial controls, storage, and voice (that were typically delivered via non-IP devices and networks) via Ethernet and TCP/IP.

DNP3

The distributed network protocol (DNP3) provides an open standard used primarily within the energy sector for interoperability between various vendors' SCADA and smart grid applications. Some protocols, such as SMTP, fit into one layer. DNP3 is a multilayer protocol and may be carried via TCP/IP (another multilayer protocol).

Recent improvements in DNP3 allow for "Secure Authentication," which addresses challenges with the original specification that could have allowed, for example, spoofing or replay attacks. DNP3 became an IEEE standard in 2010, called IEEE 1815-2010 (now deprecated). It allowed preshared keys only. IEEE 1815-2012 is the current standard; it supports public key infrastructure (PKI).

Storage protocols

Fibre Channel over Ethernet (FCoE) and Internet small computer system interface (iSCSI) are both storage area network (SAN) protocols that provide cost-effective ways to leverage existing network infrastructure technologies and protocols to interface with storage. A SAN allows block-level file access across a network, just like a directly attached hard drive.

FCoE leverages Fibre Channel, which has long been used for storage networking but dispenses with the requirement for completely different cabling and hardware. Instead, FCoE is transmitted across standard Ethernet networks. In FCoE, Fibre Channel's host bus adapters (HBAs) is able to be combined with the NIC for economies

of scale. FCoE uses Ethernet, but not TCP/IP. Fibre Channel over IP (FCIP) encapsulates Fibre Channel frames via TCP/IP.

Like FCoE, iSCSI is a SAN protocol that allows for leveraging existing networking infrastructure and protocols to interface with storage. While FCoE simply uses Ethernet, iSCSI makes use of higher layers of the TCP/IP suite for communication and is routed like any IP protocol; the same is true for FCIP. By employing protocols beyond layer 2 (Ethernet), iSCSI can be transmitted beyond just the local network. iSCSI uses logical unit numbers (LUNs) to provide a way of addressing storage across the network. LUNs are also useful for basic access control for network accessible storage.

VoIP

Voice over Internet protocol (VoIP) carries voice via data networks, a fundamental change from analog POTS, or plain old telephone service, which remains in use after over 100 years. VoIP brings the advantages of packet-switched networks, such as lower cost and resiliency, to the telephone.

Common VoIP protocols include *real-time transport protocol* (RTP), designed to carry streaming audio and video. VoIP protocols such as RTP rely upon session and signaling protocols including *session initiation protocol* (SIP, a signaling protocol) and H.323. SRTP (secure real-time transport protocol) is able to provide secure VoIP, including confidentiality, integrity, and secure authentication. SRTP uses AES for confidentiality and SHA-1 for integrity.

While VoIP can provide compelling cost advantages, especially for new sites without a large legacy voice investment, there are security concerns. Many VoIP protocols, such as RTP, provide little or no security by default.

SOFTWARE-DEFINED NETWORKS

Software-defined networking (SDN) separates a router's control plane from the data (forwarding) plane. The control plane makes routing decisions. The data plane forwards data (packets) through the router. With SDN routing, decisions are made remotely instead of on each individual router.

The most well-known protocol in this space is OpenFlow, which can, among other capabilities, allow for control of switching rules to be designated or updated at a central controller. OpenFlow is a TCP protocol that uses transport layer security (TLS) encryption.

WIRELESS LOCAL-AREA NETWORKS

Wireless local-area networks (WLANs) transmit information via light or electromagnetic waves, such as radio. The most common form of wireless data networking is the 802.11 wireless standard, and the first 802.11 standard that provides reasonable security is 802.11i.

FHSS, DSSS, and OFDM

Frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS) are two methods for sending traffic via a radio band. Some bands, like the 2.4-GHz ISM band, experience a great amount of interference; Bluetooth, some cordless phones, some 802.11 wireless, baby monitors, and even microwaves can broadcast or interfere with this band. Both DSSS and FHSS can maximize throughput while minimizing the effects of interference.

DSSS uses the entire band at once, "spreading" the signal throughout the band. FHSS uses a number of small frequency channels throughout the band and "hops" through them in pseudorandom order.

Orthogonal frequency-division multiplexing (OFDM) is a newer multiplexing method, allowing simultaneous transmissions to use multiple independent wireless frequencies that do not interfere with each other.

802.11 abgn

802.11 wireless has many standards, using various frequencies and speeds. The original mode is simply called 802.11 (sometimes *802.11-1997*, based on the year it was created), which operated at 2 megabits per second (Mbps) using the 2.4 GHz frequency. It was quickly supplanted by *802.11b*; at 11 Mbps, *802.11g* was designed to be backwards compatible with 802.11b devices, offering speeds up to 54 Mbps using the 2.4 GHz frequency. *802.11a* offers the same top speed, using the 5 GHz frequency.

802.11n uses both 2.4 and 5 GHz frequencies and is able to use multiple antennas with multiple-input multiple-output (MIMO). This allows speeds up to 600 Mbps. Finally, 802.11ac uses the 5 GHz frequency only, offering speeds up to 1.3 Gbps. Table 4.3 summarizes the major types of 802.11 wireless.

WEP

The WEP is the wired equivalent privacy protocol was an early attempt (first ratified in 1999) to provide 802.11 wireless security. WEP has proven to be critically weak, and new attacks can break any WEP key in minutes. Due to these attacks, WEP effectively provides little integrity or confidentiality protection. In fact, many consider WEP to be broken and strongly discourage its use. The encryption algorithms

Table 4.3 Types of 802.11 Wireless

Type	Top Speed	Frequency
802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	72–600 Mbps	2.4 GHz/5 GHz
802.11ac	422 Mbps–1.3 Gbps	5 GHz

specified in 802.11i and/or other encryption methods such as virtual private networks (VPNs) should be used in place of WEP.

802.11i

802.11i is the first 802.11 wireless security standard that provides reasonable security. 802.11i describes a robust security network (RSN), which allows pluggable authentication modules. RSN allows changes to cryptographic ciphers as new vulnerabilities are discovered.

CRUNCH TIME

RSN is also known as WPA2 (Wi-Fi Protected Access 2), a full implementation of 802.11i. By default, WPA2 uses AES encryption to provide confidentiality, and CCMP (counter mode CBC MAC protocol) to create a message integrity check (MIC), which provides integrity.

The less secure *WPA* (without the "2") is appropriate for access points that lack the power to implement the full 802.11i standard, providing a better security alternative to WEP. WPA uses RC4 for confidentiality and TKIP (Temporal Key Integrity Protocol) for integrity.

Bluetooth

Bluetooth, described by IEEE standard 802.15, is a PAN wireless technology, operating in the same 2.4 GHz frequency as many types of 802.11 wireless devices. Small, low-power devices such as cell phones use Bluetooth to transmit data over short distances. Bluetooth versions 2.1 and older operate at 3 Mbps or less; Versions 3 and 4 offer far faster speeds.

Sensitive devices should disable automatic discovery by other Bluetooth devices. The "security" of discovery relies on the secrecy of the 48-bit MAC address of the Bluetooth adapter. Even when disabled, Bluetooth devices are easily discovered by guessing the MAC address. The first 24 bits are the OUI, which can be easy to guess, while the last 24 bits may be determined via brute-force attack.

RFID

Radio frequency identification (RFID) is a technology used to create wirelessly readable tags for animals or objects. There are three types of RFID tags: *active, semipassive, and passive*. Active and semipassive RFID tags have a battery. An active tag broadcasts a signal, while semipassive RFID tags rely on a RFID reader's signal for power. Passive RFID tags have no battery and must rely on the RFID reader's signal for power.

SECURE NETWORK DEVICES AND PROTOCOLS

Let us look at network devices ranging from layer 1 hubs through application-layer proxy firewalls that operate up to layer 7. Many of these network devices, such as routers, have protocols dedicated to their use.

REPEATERS AND HUBS

Repeaters and hubs are layer 1 devices. A repeater receives bits on one port, and "repeats" them out the other port. The repeater has no understanding of protocols; it simply repeats bits. Repeaters can extend the length of a network.

A hub is a repeater with more than two ports. It receives bits on one port and repeats them across all other ports.

BRIDGES

Bridges and switches are layer 2 devices. A bridge has two ports and two collision domains, and it connects network segments together. Each segment typically has multiple nodes, and the bridge learns the MAC addresses of nodes on either side. Traffic sent from two nodes on the same side of the bridge will not be forwarded across the bridge. Traffic sent from a node on one side of the bridge to the other side will forward across. The bridge provides traffic isolation and makes forwarding decisions by learning the MAC addresses of connected nodes.

SWITCHES

A switch is a bridge with more than two ports. It is best practice to connect only one device per switch port. Otherwise, everything that is true about a bridge is also true about a switch.

Fig. 4.1 shows a network switch. The switch provides traffic isolation by associating the MAC address of each connected device with its port on the switch.

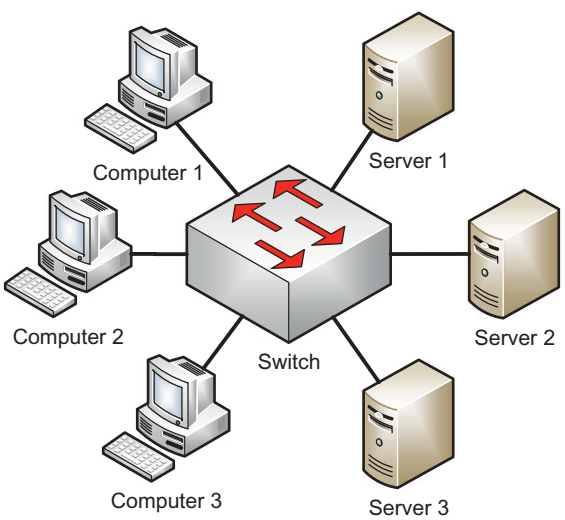

FIG. 4.1

Network switch.

A switch shrinks the collision domain to a single port. You will normally have no collisions, assuming that each port has only one connected device. Trunks connect multiple switches.

VLANs

A *VLAN* is a virtual LAN, which is like a virtual switch. Imagine you have desktops and servers connected to the same switch, and you would like to create separate desktop and server LANs. One option is to buy a second switch in order to dedicate one for desktops and one for servers. Another option is to create two VLANs, a desktop VLAN and a server VLAN, on the original switch.

One switch may support multiple VLANs, and one VLAN can span multiple switches. VLANs may also add defense-in-depth protection to networks; for example, VLANs can segment data and management network traffic.

ROUTERS

Routers are layer 3 devices that route traffic from one LAN to another. IP-based routers make routing decisions based on the source and destination IP addresses.

FIREWALLS

Firewalls filter traffic between networks. TCP/IP packet filter and stateful firewalls make decisions based on layers 3 and 4 (IP addresses and ports). Proxy firewalls can also make decisions based on layers 5–7. Firewalls are multihomed: they have multiple NICs connected to multiple different networks.

Packet filter

A *packet filter* is a simple and fast firewall. It has no concept of "state": each filtering decision is made on the basis of a single packet. There is no way to refer to past packets to make current decisions.

The packet filtering firewall shown in Fig. 4.2 allows outbound ICMP echo requests and inbound ICMP echo replies. Computer 1 can ping bank.example.com. The problem: an attacker at evil.example.com can send unsolicited echo replies, which the firewall will allow.

Stateful firewalls

Stateful firewalls have a state table that allows the firewall to compare current packets to previous ones. Stateful firewalls are slower than packet filters, but are far more secure.

Computer 1 sends an ICMP echo request to bank.example.com in Fig. 4.3. The firewall is configured to ping Internet sites, so the stateful firewall allows the traffic and adds an entry to its state table.

An echo reply is received from bank.example.com at Computer 1 in Fig. 4.3. The firewall checks to see if it allows this traffic (it does), then it checks the state table

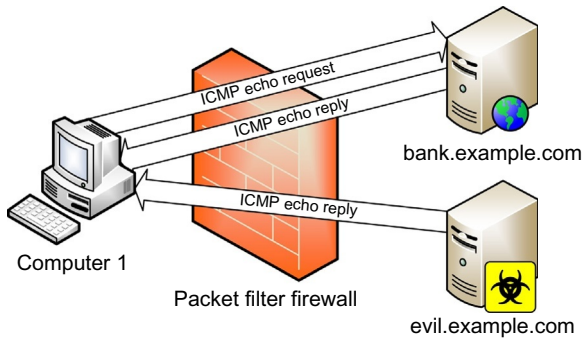

FIG. 4.2

Packet filter firewall design.

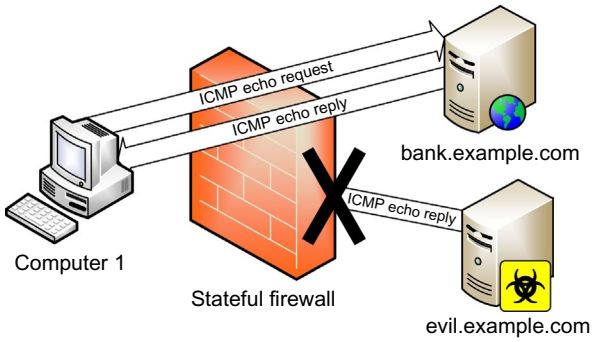

FIG. 4.3

Stateful firewall design.

for a matching echo request in the opposite direction. The firewall finds the matching entry, deletes it from the state table, and passes the traffic.

Then evil.example.com sends an unsolicited ICMP echo reply. The stateful firewall, shown in Fig. 4.3, sees no matching state table entry and denies the traffic.

Proxy firewalls

Proxies are firewalls that act as intermediary servers. Both packet filter and stateful firewalls pass traffic through or deny it; they are another hop along the route. Proxies terminate connections.

Application-layer proxy firewalls

Application-layer proxy firewalls operate up to layer 7. Unlike packet filter and stateful firewalls that make decisions based on layers 3 and 4 only, application-layer proxies can make filtering decisions based on application-layer data, such as HTTP traffic, in addition to layers 3 and 4.

MODEM

A *modem* is a modulator/demodulator. It takes binary data and modulates it into analog sound carried on phone networks designed for the human voice. The receiving modem then demodulates the analog sound back into binary data.

SECURE COMMUNICATIONS

Protecting data in motion is one of the most complex challenges we face. The Internet provides cheap global communication with little or no built-in confidentiality, integrity, or availability.

AUTHENTICATION PROTOCOLS AND FRAMEWORKS

An authentication protocol authenticates an identity claim over the network. Good security design assumes that a network eavesdropper may sniff all packets sent between the client and authentication server, so the protocol should remain secure.

802.1X and EAP

802.1X is port-based network access control (PNAC) and includes *extensible authentication protocol* (EAP). EAP is an authentication framework that describes many specific authentication protocols. EAP provides authentication at layer 2 (it is port-based, like ports on a switch) before a node receives an IP address. It is available for both wired and wireless but is more commonly deployed on WLANs. An EAP client is called a supplicant, which requests authentication to an authentication server (AS).

FAST FACTS

There are many types of EAP; we will focus on LEAP, EAP-TLS, EAP-TTLS, and PEAP:

- LEAP (*lightweight extensible authentication protocol*) is a Cisco-proprietary protocol released before 802.1X was finalized. LEAP has significant security flaws and should not be used.
- EAP-TLS (*EAP-Transport Layer Security*) uses PKI, requiring both server-side and client-side certificates. EAP-TLS establishes a secure TLS tunnel used for authentication. EAP-TLS is very secure due to the use of PKI but is complex and costly for the same reason. The other major versions of EAP attempt to create the same TLS tunnel without requiring a client-side certificate.
- EAP-TTLS (*EAP Tunneled Transport Layer Security*), developed by Funk Software and Certicom, simplifies EAP-TLS by dropping the client-side certificate requirement, allowing other authentication methods (such as passwords) for client-side authentication. EAP-TTLS is thus easier to deploy than EAP-TLS, but less secure when omitting the client-side certificate.
- PEAP (*Protected EAP*), developed by Cisco Systems, Microsoft, and RSA Security, is similar to and is a competitor of EAP-TTLS, as they both do not require client-side certificates.

VPN

Virtual private networks (VPNs secure data sent via insecure networks like the Internet. The goal is to virtually provide the privacy afforded by a circuit, such as a T1. The basic construction of VPNs involves secure authentication, cryptographic hashes such as SHA-1 to provide integrity, and ciphers such as AES to provide confidentiality.

PPP

PPP (point-to-point protocol) is a layer 2 protocol that provides confidentiality, integrity, and authentication via point-to-point links. PPP supports synchronous links, such as T1s, in addition to asynchronous links, such as modems.

IPsec

IPv4 has no built-in confidentiality; higher-layer protocols like TLS provide security. To address this lack of security at layer 3, IPsec (Internet protocol security) was designed to provide confidentiality, integrity, and authentication via encryption for IPv6. IPsec is ported to IPv4. IPsec is a suite of protocols; the major two are encapsulating security protocol (ESP) and authentication header (AH). Each has an IP protocol number; ESP is protocol 50 and AH is protocol 51.

SSL and TLS

Secure sockets layer (SSL) protects HTTP data: HTTPS uses TCP port 443. TLS is the latest version of SSL, equivalent to SSL version 3.1. The current version of TLS is 1.2.

Though initially focused on the web, SSL or TLS may be used to encrypt many types of data and can be used to tunnel other IP protocols to form VPN connections. SSL VPNs can be simpler than their IPsec equivalents: IPsec makes fundamental changes to IP networking, so installation of IPsec software changes the operating system, which requires super-user privileges. SSL client software does not require altering the operating system. Also, IPsec is difficult to firewall, while SSL is much simpler.

REMOTE ACCESS

In an age of telecommuting and the mobile workforce, secure remote access is a critical control. This includes connecting mobile users via methods such as a digital subscriber line (DSL) or cable modem, as well as newer concerns, such as instant messaging and remote meeting technology.

DSL

Digital subscriber line (DSL) has a "last mile" solution that uses existing copper pairs to provide digital service to homes and small offices.

Common types of DSL are symmetric digital subscriber line (SDSL, with matching upload and download speeds); asymmetric digital subscriber line (ADSL), featuring faster download speeds than upload speeds; and very high-rate digital subscriber line (VDSL, featuring much faster asymmetric speeds). Another option is high-data-rate DSL (HDSL), which matches SDSL speeds using two copper pairs.

Table 4.4 DSL Speed and Distances[1]

Type	Download Speed	Upload Speed	Distance from CO
ADSL	1.5–9 Mbps	16–640 Kbps	18,000 ft
SDSL	1.544 Mbps	1.544 Mbps	10,000 ft
HDSL	1.544 Mbps	1.544 Mbps	10,000 ft
VDSL	20–50 + Mbps	Up to 20 Mbps	<5000 ft

HDSL provides inexpensive T1 service. As a general rule, the closer a site is to the Central Office (CO), the faster the available service will be.

Table 4.4 summarizes the speeds and modes of DSL.

Cable modems

Cable modems are used by cable TV providers to offer Internet access via broadband cable TV. Cable TV access is not ubiquitous, but it is available in most large towns and cities in industrialized areas. Unlike DSL, cable modem bandwidth can be shared with neighbors on the same network segment.

Remote desktop console access

Two common modern protocols providing for remote access to a desktop are virtual network computing (VNC), which typically runs on TCP 5900, and remote desktop protocol (RDP), which typically runs on TCP port 3389. VNC and RDP allow for graphical access of remote systems, as opposed to the older terminal-based approach to remote access. RDP is a proprietary Microsoft protocol.

Desktop and application virtualization

Desktop virtualization is an approach that provides a centralized infrastructure that hosts a desktop image that the workforce can leverage remotely. Desktop virtualization is often referred to as VDI, which, depending on the vendor in question, stands for either virtual desktop infrastructure or virtual desktop interface.

As opposed to providing a full desktop environment, an organization can simply virtualize key applications that are centrally served. Like desktop virtualization, the centralized control associated with application virtualization allows the organization to employ strict access control and perhaps more quickly patch the application. Additionally, application virtualization can run legacy applications that would otherwise be unable to run on the systems employed by the workforce.

Screen scraping

Screen scraping presents one approach to graphical remote access to systems. Screen scraping protocols packetize and transmit information necessary to draw the accessed system's screen on the display of the system being used for remote access. VNC, a commonly used technology for accessing remote desktops, is fundamentally a screen scraping style approach to remote access. However, not all remote access

protocols are screen scrapers. For example, Microsoft's popular RDP does not employ screen scraping to provide graphical remote access.

Instant messaging

Instant messaging allows two or more users to communicate with each other via real-time "chat." Chat may be one-to-one or many-to-many, as in chat groups. In addition to chatting, most modern instant messaging software allows file sharing and sometimes audio and video conferencing.

An older instant messaging protocol is IRC (Internet relay chat), a global network of chat servers and clients created in 1988 that remains very popular even today. Other chat protocols and networks include AOL instant messenger (AIM), ICQ (short for "I seek you"), and extensible messaging and presence protocol (XMPP) (formerly known as Jabber).

Chat software may be subject to various security issues, including remote exploitation, and must be patched like any other software. The file sharing capability of chat software may allow users to violate policy by distributing sensitive documents; there are similar issues with the audio and video sharing capability of many of these programs.

Remote meeting technology

Remote meeting technology is a newer technology that allows users to conduct online meetings via the Internet, including desktop sharing functionality. These technologies usually include displaying PowerPoint slides on all PCs connected to a meeting, sharing documents such as spreadsheets, and sometimes sharing audio or video.

Many of these solutions can tunnel through outbound SSL or TLS traffic, which can often pass via firewalls and any web proxies. It is important to understand and control remote meeting technologies in order to remain compliant with all applicable policy.

PDAs

Personal digital assistants (PDAs) are small networked computers that can fit in the palm of your hand. PDAs have evolved over the years, beginning with first-generation devices such as the Apple Newton (Apple coined the term PDA) and Palm Pilot. These early PDAs offered features such as a calendar and note-taking capability. PDA operating systems include Apple iOS, Windows Mobile, Blackberry, and Google's Android, among others.

Two major issues regarding PDA security are the loss of data due to theft or loss of the device, and wireless security. Sensitive data on PDAs should be encrypted, or the device itself should store minimal amount of data. A PIN should lock the device, and the device should offer *remote wipe* capability, which is the ability to remotely erase the device in case of loss or theft.

Content distribution networks

Content distribution networks (CDN, also called content delivery networks, use a series of distributed caching servers to improve performance and lower the latency of downloaded online content. They automatically determine the servers

closest to end users, so users download content from the fastest and closest servers on the Internet. Examples include Akamai, Amazon CloudFront, CloudFlare, and Microsoft Azure.

SUMMARY OF EXAM OBJECTIVES

Communication and Network Security is a large and complex domain, requiring broad and sometimes deep understanding of thorny technical issues. Our modern world relies on networks, which must be secure. It is important understand why we use concepts like packet-switched networks and the OSI model, as well as how we implement those concepts.

Older Internet-connected networks often had a single dual-homed host connected to the Internet. Firewalls were created and then evolved from packet filter to stateful. Our physical design evolved from busses to stars, providing fault tolerance and hardware isolation. We have evolved from hubs to switches that provide traffic isolation, and we have deployed secure protocols such as TLS and IPsec.

We have improved our network defense-in-depth every step of the way, as well as increased the confidentiality, integrity, and availability of our network data.

TOP FIVE TOUGHEST QUESTIONS

1. Restricting Bluetooth device discovery relies on the secrecy of what?
   - **A.** MAC address
   - **B.** Symmetric key
   - **C.** Private key
   - **D.** Public key
2. What are the names of the OSI model layers in order from bottom to top?
   - **A.** Physical, Data Link, Transport, Network, Session, Presentation, Application
   - **B.** Physical, Network, Data Link, Transport, Session, Presentation, Application
   - **C.** Physical, Data Link, Network, Transport, Session, Presentation, Application
   - **D.** Physical, Data Link, Network, Transport, Presentation, Session, Application
3. What is the most secure type of EAP?
   - **A.** EAP-TLS
   - **B.** EAP-TTLS
   - **C.** LEAP
   - **D.** PEAP
4. What is the most secure type of firewall?
   - **A.** Packet filter
   - **B.** Stateful firewall
   - **C.** Circuit-level proxy firewall
   - **D.** Application-layer proxy firewall

5. Accessing an IPv6 network via an IPv4 network is called what?
   - **A.** CIDR
   - **B.** NAT
   - **C.** Translation
   - **D.** Tunneling

ANSWERS

1. Correct answer and explanation: A. Restricting Bluetooth device discovery relies on the secrecy of the 48-bit Bluetooth MAC address.
   Incorrect answers and explanations: Answers B, C, and D are incorrect. While E0 is a symmetric cipher, it not used to restrict discovery, though it is used for data encryption. Public or private keys are also not used for Bluetooth discovery.
2. Correct answer and explanation: C. The OSI model layers from bottom to top are: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Remember "Please Do Not Throw Sausage Pizza Away" as a useful mnemonic to remember this.
   Incorrect answers and explanations: Answers A, B, and D are incorrect. All layers are in the wrong order.
3. Correct answer and explanation: A. EAP-TLS is the most secure (and costly) form of EAP because it requires both server and client-side certificates.
   Incorrect answers and explanations: Answers B, C, and D are incorrect. EAP-TTLS and PEAP are similar and don't require client-side certificates. LEAP is a Cisco-proprietary protocol that does not require client-side certificates; it also has fundamental security weaknesses.
4. Correct answer and explanation: D. Application-layer firewalls are the most secure, as they have the ability to filter based on OSI Layers 3–7.
   Incorrect answers and explanations: Answers A, B, and C are incorrect. All are firewalls. A packet filter is the least secure of the four, due to the lack of state. A stateful firewall is more secure than a packet filter, but its decisions are limited to Layers 3 and 4. Circuit-level proxy firewalls operate at Layer 5 and cannot filter based on application-layer data.
5. Correct answer and explanation: D. Accessing an IPv6 network via an IPv4 network is called tunneling.
   Incorrect answers and explanations: Answers A, B, and C are incorrect. CIDR is Classless Interdomain Routing, a way to create flexible subnets. NAT is network address translation, which translates one IP address for another. Translation is a distractor answer.

ENDNOTE

1. DSL and Cable Modem Networks, http://www.ciscopress.com/articles/article.asp?p=31289 (accessed 25.04.16).